Volker Roth

Rechnersicherheit, SoSe 21

Übung 03

TutorIn: Oliver Wiese
Tutorium 02
Materialien: Latex, VSC, Skript

30. Juni 2021

---

1 SA and EM

In class we discussed static analysis and execution monitors. We like to recap and discuss some concepts.

(a) *Discuss differences between safety and liveness properties.*

- Safety stipulate that “bad things never happen” during execution.
- in contrast to liveness properties which stipulate that, eventually, “good things will happen” during execution.

(b) *Discuss differences between SA and EM mechanisms.*

- A SA mechanism takes a program a and decides if it fits the policy, afterwards it returns a program. If it does, the initial program a is returned. Else a different program is returned, which halts on every input.
- A EM mechanism takes a program a and returns a created program b. b runs a and observes in the run time if a violates the policy. If it does, b halts. b can only observe a single execution of a.
- So SA happens befor runtime and EM in runtime
- Also Every SA mechanism is also enforceable by an EM mechanism, but not the contrary.

(c) *Give a practical example of SA mechanisms.*

- type-safe for program languages (such as Java)
- standard virus scanners

(d) *Give a practical example of EM mechanisms.*

- Software testing (memory leaks, out-of-bounds array accesses, race conditions, atomicity, etc.)
- Auditing and Logging

2 Security Policies in our Project

In class we discussed security policies in a very formal way. In this exercise we focus on some practical aspects of security policies in context of your project (chat server and client).

(a) *Give three relevant security policies for your project. The description of security policies can be informal.*

1. Users should not be able to see whenever a new user connected or disconnected from the server
2. User should not be able to change any data in the programm (code)
3. Policies for different account privileges. (Admins can delete msgs, while users are unable to)

(b) *For each above security policy: Who should enforce the policy? The operating system, your program or someone else?*

1. The 1st and 3rd policies are somewhat similar; both could also be implemented in code. For 1. simply omit the option, and for 3. restrict the option to admin accounts.
2. 2. Should be handled by the operating system.

(c) *For each security policy: How can be your security policies enforced? With a SA or EM mechanism?*

- We'd choose for every policy a EM mechanims. (Especially because an em mechanism can simulate an sa mechanism :)